ESSENTIAL DIMENSION AND LINEAR CODES

SHANE CERNELE

Abstract. One of the central open problems in the theory of essential dimension is to compute the essential dimension of PGL$_n$, whose torsors correspond to central simple algebras up to isomorphism. In this paper, we study the essential dimension of groups of the form $G/\mu$, where $G$ is a reductive algebraic group satisfying certain properties, and $\mu$ is a central subgroup of $G$. The Galois cohomology of $G/\mu$ is studied in the Appendix by Athena Nguyen.

In particular, we consider the case

$$G = \text{GL}_{n_1} \times \cdots \times \text{GL}_{n_r}$$

where each $n_i$ is a power of a single prime $p$, which is a generalization of the group $\text{PGL}_{p^a} = \text{GL}_{p^a} / \mathbb{G}_m$. In this example, the first Galois cohomology set $H^1(K, G/\mu)$ corresponds to tuples of central simple $K$-algebras satisfying certain conditions.

Surprisingly, computing the essential dimension of $G/\mu$ becomes easier when $r \geq 3$. In this paper we give upper and lower bounds for the essential dimension of $G/\mu$, and in some cases we determine the exact value.

1. Introduction

1.1. Background. Informally, the essential dimension of an object is the minimum number of algebraically independent variables required to define that object. Essential dimension was introduced by Buhler and Reichstein ([BR97]) in 1997, and the definition has since been generalized by Reichstein ([R00]) and Merkurjev ([BF03]). For the definition and further background on essential dimension, see the recent surveys [R10] and [M13].

Let $k$ be a base field of characteristic zero. Computing the essential dimension of PGL$_n$, which equals the maximum essential dimension of a central simple algebra of degree $n$, is one of the central open problems in the theory of essential dimension. For $n \geq 5$ and odd, from [LRRS03] we have

$$\text{ed}_k(\text{PGL}_n) \leq \frac{1}{2}(n-1)(n-2)$$

and if $a^b \mid n$ for some $a > 1$, from [R00] Theorem 9.3 & Proposition 9.8a] we have

$$\text{ed}_k(\text{PGL}_n) \geq 2b$$

Stronger results are known for a ‘local version’ of essential dimension at a prime $p$, called essential $p$-dimension. In this case if $n = p^ab$ with $(p, b) = 1$ then

$$\text{ed}_k(\text{PGL}_n; p) = \text{ed}_k(\text{PGL}_{p^a}; p)$$

and so we can reduce to studying only central simple algebras of $p$-primary degree.

Every central simple algebra of index $p$ becomes a cyclic algebra after a prime-to-$p$ extension of the base field; from this one can deduce

$$\text{ed}_k(\text{PGL}_p; p) = 2$$

2010 Mathematics Subject Classification. Primary 20G15, Secondary 16K20.

This paper is based on the author’s PhD thesis completed at the University of British Columbia. The author gratefully acknowledges financial support from the Natural Sciences and Engineering Research Council of Canada and the University of British Columbia.
(see [RY00 Lemma 8.5.7]). When \( a \geq 2 \) we have the following result:

\[
(a - 1)p^a + 1 \leq \text{ed}_k(\text{PGL}_{p^a}; p) \leq p^{2a-2} + 1
\]

The lower bound is from [M10] and the upper bound is from [Ru11].

The set \( H^1(K, G) \) where \( G = \text{GL}_{p^a} / \mu_{p^s} \) \((s < a)\) corresponds to central simple algebras of degree \( p^a \) and exponent dividing \( p^s \). The essential \( p \)-dimension of \( \text{GL}_{p^a} / \mu_{p^s} \) was studied in [BM12], where the authors show:

\[
\text{ed}_k(\text{GL}_{p^a} / \mu_{p^s}; p) \leq 2p^{2a-2} - p^a + p^{a-s}
\]

In this paper we will study the essential dimension of a certain class of groups, including the groups \( G/\mu \) where \( G = \text{GL}_{p^a_1} \times \ldots \times \text{GL}_{p^a_r} \) for some prime \( p \) and \( \mu \leq Z(G) \). The Galois cohomology of \( G/\mu \) is related to \( r \)-tuples of central simple algebras; see the Appendix. Surprisingly, computing the essential dimension becomes easier when \( r \geq 3 \).

Let \( C_\mu \) be the submodule of \( \mathbb{Z}^r \) consisting of all \( r \)-tuples \((x_1, \ldots, x_r) \in \mathbb{Z}^r \) such that \( \lambda_1^{x_1} \cdots \lambda_r^{x_r} = 1 \) for all \((\lambda_1, \ldots, \lambda_r) \in \mu \). Let \( \overline{C_\mu} \) be the (finite) image of \( C_\mu \) under the natural surjection

\[
\mathbb{Z}^r \rightarrow \mathbb{Z}/p^{a_1} \mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r} \mathbb{Z}
\]

If \((c_1, \ldots, c_r) \in \overline{C_\mu} \) then write \( c = (u_1p^{k_1}, \ldots, u_rp^{k_r}) \) with \( u_i \in (\mathbb{Z}/p^{a_i} \mathbb{Z})^* \) and \( 0 \leq k_i \leq a_i \), and define the ‘weight of \( c \)’, denoted \( w(c) \), by

\[
w(c) = \sum_{i=1}^r (a_i - k_i).
\]

The main result of this paper is the following. Let \( \{Y_1, \ldots, Y_t\} \) be a generating set of \( \overline{C_\mu} \) such that \( \sum_{i=1}^t w(Y_i) \) is minimal. Let \( M = \sum_{i=1}^t p^{w(Y_i)} \). Then

\[
\text{ed}_k(G/\mu) \geq M + (r - t) - p^{2a_1} - \ldots - p^{2a_r}
\]

and for many choices of \( \mu \) (when \( r \geq 3 \)), equality holds.

1.2. Notation. We will now introduce some notation before stating our main results. The major notation is summarized in the tables throughout this section. We begin by defining some standard notation in the table below.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k )</td>
<td>Base field of characteristic zero.</td>
</tr>
<tr>
<td></td>
<td>All groups and fields are defined over ( k ).</td>
</tr>
<tr>
<td>( p )</td>
<td>Positive prime integer.</td>
</tr>
</tbody>
</table>

Continued on next page...
Table 1: General Notation (continued)

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Z(B) )</td>
<td>Center of the group ( B ).</td>
</tr>
<tr>
<td>( X(A) )</td>
<td>Character lattice of the diagonalizable group ( A ).</td>
</tr>
<tr>
<td>( \text{Br}(K) )</td>
<td>Brauer group of the field ( K ).</td>
</tr>
<tr>
<td>( H^j(K, B) )</td>
<td>( j )th Galois cohomology group of ( B ) over ( K ).</td>
</tr>
</tbody>
</table>

We now proceed to define the groups and maps we will study in this paper. For \( i = 1, \ldots, r \), let \( G_i \) be a reductive linear algebraic group with \( Z(G_i) \leq \mathbb{G}_m \). In other words, we are once and for all identifying \( Z(G_i) \) with a subgroup of \( \mathbb{G}_m \), so that we may have the identity character: \( Z(G_i) \hookrightarrow \mathbb{G}_m \).

Denote \( \overline{G}_i = G_i/Z(G_i) \) and consider \( \delta_K : H^1(K, \overline{G}_i) \rightarrow H^2(K, Z(G_i)) \leq \text{Br}(K) \) for any \( K/k \). Here \( \delta_K \) is the coboundary map induced from the sequence

\[
1 \rightarrow Z(G_i) \rightarrow G_i \rightarrow \overline{G}_i \rightarrow 1
\]

for any \( K/k \), see [S97, Section I.5].

We will assume that for all \( i \) and any \( K/k \) the image of \( \delta_K \) consists of elements of \( p \)-primary order for some prime \( p \). Let \( p^{a_i} \) be the maximal index of \( \delta_K(E) \) (over all \( K/k \) and \( E \in H^1(K, \overline{G}_i) \)), and let \( p^{b_i} \) be the maximal exponent of \( \delta_K(E) \) (over all \( K/k \) and \( E \in H^1(K, \overline{G}_i) \)). We make the following additional assumptions:

i) For each \( i \), \( b_i \in \{1, a_i\} \).

ii) Either \( Z(G_i) = \mathbb{G}_m \) for all \( i \), or \( Z(G_i) = \mu_{p^{b_i}} \) for all \( i \). In particular, \( Z(G_1) \times \cdots \times Z(G_r) \) is either connected or finite.

Let \( n_i = p^{a_i} \).

**Example 1.1.** Examples of groups \( G_i \) satisfying \( b_i \in \{1, a_i\} \) and having \( Z(G_i) \in \{\mathbb{G}_m, \mu_{p^{b_i}}\} \) include:

a) \( \text{GL}_{n_i} \) and \( \text{SL}_{n_i} \) for \( p \) arbitrary, \( a_i \geq 1 \) (\( b_i = a_i \)). In this case \( \overline{G}_i = \text{PGL}_{n_i} \), and \( H^1(K, \text{PGL}_{n_i}) \) classifies central simple algebras of degree \( n_i \) over \( K \). The coboundary map sends a central simple algebra to its Brauer class in \( \text{Br}(K) \).

b) For \( p = 2 \), \( \text{GO}_{n_i}, \text{O}_{n_i}, \text{GSP}_{n_i}, \) and \( \text{SP}_{n_i} \) when \( a_i \geq 1 \) (\( b_i = 1 \)), and \( \text{GO}_{n_i}^\pm \) and \( \text{SO}_{n_i} \) when \( a_i \geq 2 \) (\( b_i = 1 \)). In these cases \( H^1(K, \overline{G}_i) \) classifies central simple algebras of degree \( n_i \) with involution (of the first kind) satisfying certain properties. The coboundary map sends a central simple algebra \( A \) with involution to the Brauer class of \( A \) in \( \text{Br}(K) \) (see [KMRT98, Section 29]). Note that if \( G_i = \text{GO}_{n_i}, \text{O}_{n_i} \) or \( \text{SO}_{n_i} \) for \( n \) odd, then the coboundary map is trivial.

c) \( E_6 \) (simply connected) for \( p = 3, a_i = 3 \) (\( b_i = 1 \)).

d) For \( p \) odd, \( \text{Spin}_{n_i} \) where \( a_i = 2^{(n-1)/2} \) (see [M96, Section 4.2]), \( b_i = 1 \). In this case \( \overline{G}_i = \text{SO}_{n_i} \), and \( H^1(K, \text{SO}_{n_i}) \) classifies quadratic forms over \( K \) of degree \( n_i \) with trivial discriminant. The coboundary map sends a quadratic form to its Hasse-Witt invariant.
e) Non-abelian finite $p$-groups $G_i$ where $Z(G_i) \cong \mu_p$ and the dimension of a minimal faithful representation of $G_i$ is $n_i$ (see [KM08, Theorem 4.4]). In this case, $a_i \geq 1$ and $b_i = 1$.

We summarize the notation related to the groups $G_i$ in the table below.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r$</td>
<td>Positive integer.</td>
</tr>
<tr>
<td>$G_i$</td>
<td>Reductive linear algebraic group with $Z(G_i) \leq \mathbb{G}_m$.</td>
</tr>
<tr>
<td>$\overline{G}_i$</td>
<td>$G_i/Z(G_i)$.</td>
</tr>
<tr>
<td>$\delta^i_K$</td>
<td>The coboundary map $H^1(K, \overline{G}_i) \to H^2(K, Z(G_i))$ induced from the sequence $1 \to Z(G_i) \to G_i \to \overline{G}_i \to 1$. We assume every element of $\text{im}(\delta^i_K)$ has $p$-primary order.</td>
</tr>
<tr>
<td>$a_i$</td>
<td>Maximum index of an element in $\text{im}(\delta^i_K)$ over all $K/k$.</td>
</tr>
<tr>
<td>$b_i$</td>
<td>Maximum exponent of an element in $\text{im}(\delta^i_K)$ over all $K/k$. We assume $b_i \in {1, a_i}$. If $</td>
</tr>
<tr>
<td>$n_i$</td>
<td>$p^{a_i}$.</td>
</tr>
</tbody>
</table>

We now proceed to define the groups whose essential dimension we are interested in, and some of their related structures. Let

$$G = G_1 \times \cdots \times G_r, \quad \text{and} \quad \overline{G} = G/Z(G) = \prod_{i=1}^{r} \overline{G}_i.$$ 

Let $\mu$ be a subgroup of $Z(G)$ (in particular, $\mu \leq \mathbb{G}_m^r$), and let

$$\delta_K : H^1(K, \overline{G}) \to H^2(K, Z(G)/\mu)$$

be the coboundary map induced from the sequence $1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$. We will compute bounds on the essential dimension of $G/\mu$ over $k$.

From $\mu \leq Z(G)$ we get a surjective map $X(Z(G)) \to X(\mu)$ given by restricting a character of $Z(G)$ to $\mu$. We define

$$C_\mu = \ker (X(Z(G)) \to X(\mu))$$

and observe that $C_\mu \cong X(Z(G)/\mu)$. 
Note that \( X(Z(G)) \) is a \( \mathbb{Z} \)-module of rank \( r \), and comes with a canonical coordinate system. This coordinate system is determined by \( r \) generators, which are the \( r \) maps \( Z(G) \to Z(G_i) \to G_m \). Thus we can think of an element of \( C_\mu \) as an \( r \)-tuple \( (z_1, \ldots, z_r) \), where

\[
z_i \in \begin{cases} 
\mathbb{Z} & \text{if } Z(G_i) \cong \mathbb{G}_m \\
\mathbb{Z}/p^b_i \mathbb{Z} & \text{if } Z(G_i) \cong \mathbb{G}_{p_i^b} 
\end{cases}
\]

and we can write \( C_\mu \) explicitly as:

\[
C_\mu = \{(c_1, \ldots, c_r) \in X(Z(G)) \mid \lambda_1^{c_1} \cdots \lambda_r^{c_r} = 1 \text{ for all } (\lambda_1, \ldots, \lambda_r) \in \mu\}.
\]

Set \( F = \mu_{p^b_1} \times \cdots \times \mu_{p^b_r} \leq Z(G) \). Given \( \mu \leq Z(G) \), we define the code associated to \( \mu \), denoted \( \overline{C_\mu} \), to be the image of \( C_\mu \) under the natural surjection \( X(Z(G)) \to X(Z(G) \cap F) \). In other words, \( \overline{C_\mu} \) is the code given by reducing the \( i^{th} \) coordinate in each element of \( C_\mu \) modulo \( p^b_i \). Note that this construction is trivial in the case where \( |Z(G)| < \infty \), since in this case we assumed \( Z(G) = F \) and hence \( C_\mu = \overline{C_\mu} \).

**Remark 1.2.** By Corollary 6.4 in the Appendix, the essential dimension of \( G/\mu \) depends only on \( \overline{C_\mu} \). In particular, if \( \mu, \tau \leq Z(G) \) with \( \overline{C_\mu} = \overline{C_\tau} \) then \( \ed_k(G/\mu) = \ed_k(G/\tau) \).

We will now assign ‘weights’ to the elements of our code. Let \( \mu \leq Z(G) \) with associated code \( \overline{C_\mu} \). Define a map \( v_i : \mathbb{Z}/p^b_i \mathbb{Z} \to \mathbb{Z} \) as follows. For \( z \in \mathbb{Z}/p^b_i \mathbb{Z} \), if \( z = 0 \) then define \( v_i(z) = a_i \). Otherwise, write \( z = up^k \) with \( u \) invertible in \( \mathbb{Z}/p^b_i \mathbb{Z} \) and \( 0 \leq k < b_i \), and define \( v_i(z) = k \).

For an element \( z = (z_1, \ldots, z_r) \in \overline{C_\mu} \), we define the weight of \( z \), denoted \( w(z) \) to be:

\[
w(z) = \sum_{i=1}^{r} (a_i - v_i(z_i))
\]

**Remark 1.3.** In the case where \( b_i = 1 \) for all \( i \), the code \( \overline{C_\mu} \) is a linear error-correcting code over \( \mathbb{F}_p \) in the traditional sense. If also \( a_1 = a_2 = \cdots = a_r \) then the weight on \( \overline{C_\mu} \) will just be \( a_1 \) times the usual Hamming weight.

**Remark 1.4.** Since we assumed \( b_i \in \{1, a_i\} \), our weight function has the following important property. Suppose that for \( i = 1, \ldots, r \), \( E_i \) is a central simple algebra with index \( p^{a_i} \) and exponent \( p^{b_i} \), and \( z_i \in \mathbb{Z}/p^b_i \mathbb{Z} \). Then \( \ind(E_i^{\otimes z_i}) = p^{a_i - v_i(z_i)} \), and further if \( z = (z_1, \ldots, z_r) \in \overline{C_\mu} \) then

\[
\ind(E_1^{\otimes z_1} \otimes \cdots \otimes E_r^{\otimes z_r}) \leq \prod_{i=1}^{r} \ind(E_i^{\otimes z_i}) = p^{w(z)}
\]

We summarize the notation related to the group \( G/\mu \) and the code associated to \( \mu \) in the following table.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G )</td>
<td>( G_1 \times \cdots \times G_r ).</td>
</tr>
<tr>
<td></td>
<td>We assume ( Z(G) ) is finite or connected.</td>
</tr>
</tbody>
</table>

Continued on next page...
Table 3: Notation Related to $G$ and $\mu$ (continued)

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\overline{G}$</td>
<td>$G/Z(G)$.</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Subgroup of $Z(G)$.</td>
</tr>
</tbody>
</table>
| $C_\mu$ | The $\mathbb{Z}$-module given by $\ker (X(Z(G)) \to X(\mu))$. Explicitly, $C_\mu$ is given by:
\[
\begin{cases}
(c_1, \ldots, c_r) \in X(Z(G)) \mid \lambda_1^{c_1} \cdot \ldots \cdot \lambda_r^{c_r} = 1, \\
\forall (\lambda_1, \ldots, \lambda_r) \in \mu
\end{cases}
\]
| $\overline{C_\mu}$ | Image of $C_\mu$ under the map $X(Z(G)) \to X(\mu_1 \times \cdots \times \mu_r)$ induced from $\mu_1 \times \cdots \times \mu_r \hookrightarrow Z(G)$. Equivalently, $\overline{C_\mu}$ is the $\mathbb{Z}$-module given by reducing the $i^{th}$ coordinate of $C_\mu$ modulo $p^b_i$, for $i = 1, \ldots, r$. $\overline{C_\mu}$ is called the code associated to $\mu$. |
| $w$ | $w : \overline{C_\mu} \to \mathbb{Z}$
\[
(u_1 p^{k_1}, \ldots, u_r p^{k_r}) \mapsto \sum_{u_i p^{k_i} \neq 0} (a_i - k_i)
\]
Here, $u_i \in (\mathbb{Z}/p^b_i \mathbb{Z})^*$ and $0 \leq k_i \leq b_i$. |
| $\delta_K$ | The coboundary map $H^1(K, G) \to H^2(K, Z(G)/\mu)$ induced from the sequence $1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$. |

1.3. Main Results. A generator matrix $Y$ of a code is a matrix whose rows generate the code, and if $Y$ is a generator matrix, then $Y_i$ denotes the $i^{th}$ row of the matrix and $y_{ij}$ denotes the entry in the $i^{th}$ row and $j^{th}$ column.

Definition 1.5. Let $Y$ be a generator matrix for $\overline{C_\mu}$, with rows $Y_1, \ldots, Y_l$. We say that $Y$ is minimal if, for any other generator matrix $Z$ of $\overline{C_\mu}$ with rows $Z_1, \ldots, Z_l$,
\[
\sum_{i=1}^l w(Y_i) \leq \sum_{i=1}^l w(Z_i).
\]

We can now state upper and lower bounds on the essential dimension of $G/\mu$, where $\mu \leq Z(G)$. Recall that, by Corollary 6.4, we are free to replace $\mu$ with any $\tau \leq Z(G)$ such that $\overline{C_\mu} = \overline{C_\tau}$. 
Theorem 1.6. Let $\mu \leq Z(G)$ and let $Y$ be a minimal generator matrix for $C_{\mu}$ with rows $Y_1, \ldots, Y_t$.

1. $ed_k(G/\mu; p) \geq \left( \sum_{i=1}^{t} p^{w(Y_i)} \right) - d - \dim(G)$
2. $ed_k(G/\mu) \leq \left( \sum_{i=1}^{t} p^{w(Y_i)} \right) - d + ed_k(G)$

where $d = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Although the upper and lower bounds in Theorem 1.6 never meet, for many families of subgroups $\mu$ the term $\sum_{i=1}^{t} p^{w(Y_i)}$ appearing in both the upper and lower bound is much larger than any of the other terms in either formula.

Definition 1.7. Let $Y$ be a matrix such the entries in the $i^{th}$ column are elements of $Z/pb_i Z$. We say that $Y$ is very acceptable if:

1. Each $y_{ij}$ equals $-1, 0$ or $1$ in $Z/pb_i Z$.
2. $Y$ contains no column of all zeroes.
3. For each $i$, the Hamming weight of $Y_i$ is at least $f(p)$, where

$$f(p) = \begin{cases} 5, & \text{if } p = 2 \\ 4, & \text{if } p = 3 \\ 3, & \text{otherwise} \end{cases}$$

When $G_i$ has a faithful representation of dimension $n_i$ such that $Z(G_i)$ acts by the identity character (for example, every $G_i$ in Example 1.1), we can sometimes use very acceptable generator matrices to find a stronger upper bound.

Theorem 1.8. Suppose that $G_i$ has a faithful representation of dimension $n_i$ such that $Z(G_i)$ acts by the identity character, for all $i$. Suppose additionally that for all $1 \leq i, j, k \leq r$, we have $a_i < a_j + a_k$ (or equivalently, $n_i < n_j \cdot n_k$). Let $\mu \leq Z(G)$ and suppose there exists a very acceptable minimal generator matrix $Y$ for $C_{\mu}$ with rows $Y_1, \ldots, Y_t$. Then

$$ed_k(G/\mu) = ed_k(G/\mu; p) = \left( \sum_{i=1}^{t} p^{w(Y_i)} \right) - d - \dim(G)$$

where $d = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Remark 1.9. Every code has a minimal generator matrix, but not every code has a very acceptable generator matrix, and even codes with very acceptable generator matrices may not have a minimal very acceptable generator matrix. Thus the bounds in Theorem 1.6 apply to all subgroups $\mu$, whereas the formula in Theorem 1.8 only applies in certain cases, even if one assumes the groups $G_i$ and the integers $a_i$ satisfy the additional hypotheses of Theorem 1.8.

Note that if $a_1 = \ldots = a_r$ and either $p^{b_1} = \ldots = p^{b_r} = 2$ or $p^{b_1} = \ldots = p^{b_r} = 3$, then the definition of very acceptable and the additional hypotheses in Theorem 1.8 can be simplified. In these cases, $C_{\mu}$ will have a very acceptable minimal generator matrix and Theorem 1.8 will apply if:

1. $G_i$ has a faithful representation of dimension $n_i$ such that $Z(G_i)$ acts by the identity character for all $i$. 


(2) For $1 \leq i \leq r$, $C_\mu$ contains an element whose $i^{th}$ coordinate is non-zero.

(3) The minimum Hamming weight of $C_\mu$ is at least 5 (if $p^{b_i} = 2$ for all $i$) or 4 (if $p^{b_i} = 3$ for all $i$).

**Remark 1.10.** The conditions in Theorem 1.8 that for all $1 \leq i, j, k \leq r$, $a_i < a_j + a_k$, and that $Y$ is very acceptable can be replaced by assuming $Y$ is an acceptable generator matrix. The definition of an acceptable generator matrix is more complicated to describe; see Section 4.

**Example 1.11.** A motivating example to keep in mind is the following. Let $n_1 = n_2 = \cdots = n_r = p^a$ for $r \geq 5$ and $a \geq 1$, and let $G_i \cong \text{GL}_{n_i}$ for $1 \leq i \leq r$. Let $\mu < Z(G)$ be defined by:

$$\mu := \{(\lambda_1, \ldots, \lambda_r) \in Z(G) \mid \lambda_1 \cdot \cdots \cdot \lambda_r = 1\}$$

Thus $C_\mu = \langle (1, 1, \ldots, 1) \rangle \leq X(Z(G)) = \mathbb{Z}^r$. By Theorem 1.8, we have

$$\text{ed}_k(G/\mu) = \text{ed}_k(G/\mu;p) = p^{rn} - rp^2 + r - 1$$

See Section 5 for a generalization of this example.

The rest of this report is structured as follows. In Section 2, we will discuss codes and minimal generator matrices, and in Section 3 we discuss the relationship between codes and subgroups of the Brauer group to prove Theorem 1.6. In Section 4 we prove Theorem 1.8 and we conclude in Section 5 with an interesting example. The Appendix, written by Athena Nguyen, studies the Galois cohomology of $G/\mu$ in the case where $Z(G)$ is connected. Throughout, all diagrams are commutative, $G$ and $\overline{G}$ are groups of the form described in this section, and $\mu$ denotes a subgroup of $Z(G)$.

**Acknowledgements.** I would like to thank Zinovy Reichstein for his many helpful discussions on earlier versions of this paper, and for showing me the proof of Theorem 6.3. Also, I am grateful to Zinovy Reichstein and Roland L"otcher for helpful suggestions regarding the proof of the lower bound in Theorem 1.8. I would also like to thank Lior Silberman for his helpful comments and questions, Athena Nguyen for showing me the results which are now described in the Appendix of this paper, and Mario Garcia Armas and Jerome Lefebvre for helpful conversations.

I am grateful to BIRS and the organizers of the 2012 conference ‘Lie algebras, torsors and cohomological invariants’, where some of this research was conducted.

## 2. On Minimal Generator Matrices

The $\mathbb{Z}$-module $C_\mu$ can be thought of as a $\mathbb{Z}/p^b\mathbb{Z}$-module, where $b := \max\{b_1, \ldots, b_r\}$. In this section we will develop some preliminary algebraic results for this context. In particular, we show in Example 2.8 that if we replaced our weight function $w$ with the weight function $p^w$, then the set of minimal generator matrices would remain unchanged. We assume for simplicity that generating sets are ordered and do not contain 0.

Let $R$ be a local ring, $I$ the unique maximal ideal of $R$, and let $M$ be a finitely generated $R$-module. For $m \in M$, let $\overline{m}$ denote the image of $m$ in $M/IM$. The following lemma can be deduced from Nakayama’s Lemma, and is an immediate consequence of [AM69 Proposition 2.8].

**Lemma 2.1.** The set $\{m_1, \ldots, m_t\}$ is a generating set of minimal size for $M$ as an $R$-module if and only if $\overline{m_1}, \ldots, \overline{m_t}$ is a basis for $M/IM$ as an $R/I$-vector space.

Let $w : M \rightarrow \mathbb{Z}_{\geq 0}$ be a function with $w(m) \neq 0$ if $m \neq 0$. For each generating set $B = \{m_1, \ldots, m_t\}$ of $M$, we define

$$w(B) := (w(m_1), \ldots, w(m_t), 0, 0, \ldots) \in \mathbb{Z}^N$$

We define $w_{\text{ord}}(B)$ to be the element of $\mathbb{Z}^N$ obtained by rearranging the entries of $w(B)$ in decreasing order, and we call $w_{\text{ord}}(B)$ the $w$-profile of $B$. 

Remark 2.2. If \( B \) is arranged in weight-decreasing order, then \( w_{\text{ord}}(B) = w(B) \).

If \( \gamma \) is a \( w \)-profile of \( M \), we call a generating set \( B_\gamma = \{ \beta_1, \ldots, \beta_t \} \) a \textit{representative generating set} for \( \gamma \) if the \( w \)-profile of \( B_\gamma \) equals \( \gamma \).

We put a partial order \( \leq \) on \( \mathbb{Z}^N \) as follows. For \( \gamma, \beta \in \mathbb{Z}^N \), \( \gamma \leq \beta \) if \( \gamma_i \leq \beta_i \) for all \( i \geq 1 \), where \( \gamma_i \) denotes the \( i^{th} \) component of \( \gamma \in \mathbb{Z}^N \). Let \( \text{Prof}(M) \) (or, \( \text{Prof}_w(M) \)) denote the set of \( w \)-profiles of generating sets of \( M \).

Theorem 2.3. \( (\text{Prof}(M), \leq) \) has a unique minimal element, and this element is comparable to every other element.

Proof. \( \text{Prof}(M) \) has no infinite descending totally ordered chain, so it suffices to show that there is a unique minimal element. Towards a contradiction, suppose \( X \) and \( Y \) are representative generating sets for distinct minimal elements of \( \text{Prof}(M) \). By Lemma 2.1, both \( X \) and \( Y \) must have the same size, say \( t \). Thus write \( X = \{ x_1, \ldots, x_t \} \) and \( Y = \{ y_1, \ldots, y_t \} \) with \( w(x_1) \geq \cdots \geq w(x_t) \) and \( w(y_1) \geq \cdots \geq w(y_t) \). Suppose \( s \) is minimal such that \( w(x_i) = w(y_i) \) for all \( i > s \). Since \( s \geq 1 \) and \( X \) and \( Y \) are distinct, we have \( w(x_s) < w(y_s) \).

We can extend the set \( \{ x_s, \ldots, x_t \} \) to a minimal generating set of \( M \) by adding elements of \( Y \). That is, for some \( J = \{ j_1, \ldots, j_{s-1} \} \subset Y \) with \( w(j_1) \geq w(j_2) \geq \cdots \geq w(j_{s-1}) \), we have that

\[
\{ j_1, \ldots, j_{s-1}, x_s, \ldots, x_t \}
\]

is a basis for \( M/IM \) as an \( R/I \)-vector space. By Lemma 2.1,

\[
\Gamma := \{ j_1, \ldots, j_{s-1}, x_s, \ldots, x_t \}
\]

generates \( M \) as an \( R \)-module.

We will now compare the weights of the elements of \( \Gamma \) with the weights of the elements of \( Y \). By construction, \( w(x_i) = w(y_i) \) for \( s+1 \leq i \leq t \), and \( w(x_s) < w(y_s) \) by assumption. Since \( J \) is an ordered subset of \( Y \) and \( w(y_1), \ldots, w(y_{s-1}) \) are the largest \( s-1 \) weights of elements in \( Y \), we have \( w(j_i) \leq w(y_i) \) for \( 1 \leq i \leq s-1 \). Thus we have \( w(\Gamma) < w(Y) = w_{\text{ord}}(Y) \). It remains to show that \( w_{\text{ord}}(\Gamma) < w_{\text{ord}}(Y) \), since this would contradict the minimality of \( Y \).

Let \( j_i = x_i \) for \( s \leq i \leq t \) so that we may write

\[
\Gamma := \{ j_1, \ldots, j_{s-1}, j_s, \ldots, j_t \}.
\]

If there exists \( a, b \) with \( a < b \) such that \( w(j_a) < w(j_b) \), then we swap these two elements to get a new generating set \( \Gamma' \). We must show that \( w(\Gamma') < w_{\text{ord}}(Y) \), since then after finitely many such swaps we obtain a generating set \( \Gamma'' \), which is just \( \Gamma \) rearranged into weight-decreasing order. Thus inductively we would have \( w(\Gamma'') < w_{\text{ord}}(Y) \), and hence:

\[
 w_{\text{ord}}(\Gamma) = w_{\text{ord}}(\Gamma'') = w(\Gamma'') < w_{\text{ord}}(Y).
\]

Note that the first inequality is true because \( \Gamma \) and \( \Gamma'' \) contain the same elements, and the second equality follows from Remark 2.2.

Since \( \Gamma \) only changes in positions \( a \) and \( b \), it is enough to show that \( w(j_b) \leq w(y_a) \) and \( w(j_a) < w(y_b) \) (note that the second inequality is automatically strict). Since \( w(\Gamma) < w(Y) \), we have \( w(j_a) \leq w(y_a) \) and \( w(j_b) \leq w(y_b) \), and since \( Y \) is in decreasing order, we have \( w(y_b) \leq w(y_a) \). Thus the first inequality follows from \( w(j_b) \leq w(y_b) \leq w(y_a) \), and the second inequality follows from \( w(j_a) < w(y_b) \leq w(y_a) \). \( \square \)

Corollary 2.4. A generating set \( B = \{ m_1, \ldots, m_l \} \) of \( M \) minimizes \( \sum_{i=1}^{l} w(m_i) \) if and only if \( w_{\text{ord}}(B) \) is the minimal element of \( \text{Prof}(M) \).
Corollary 2.5. Suppose we form a generating set of $M$ inductively as follows: Select $m_1 \in M$ with $m_1 \neq 0 \in M$ such that $w(m_1)$ is minimal. Suppose $m_1, \ldots, m_t$ have been selected. Then select $m_{t+1}$ such that $w(m_{t+1})$ is minimal among all elements $m \in M$ such that $m \notin (m_1, \ldots, m_t)$. Continue until it is not possible to select another element. Then the $w$-profile of the resulting generating set is the minimal element of $\text{Prof}(M)$.

Example 2.6. [KM08, Remark 4.7] Take $R = \mathbb{F}_p$, $G$ a finite $p$-group, $D$ to be the elements of exponent at most $p$ in $Z(G)$ and $M = X(D)$, where $X(D)$ is the group of characters of $D$. For $x \in M$, define $w(x)$ to be the least dimension of a representation of $G$, say $V_x$, such that $D$ acts by $x$. Then if $\{x_1, \ldots, x_i\}$ is the basis provided by the greedy algorithm in Corollary 2.5, then $V_{x_1} \oplus \cdots \oplus V_{x_i}$ is a faithful representation of $G$ of minimal dimension.

Corollary 2.7. Suppose $\tau : M \to \mathbb{Z}_{\geq 0}$ is a function, with $\tau(m) \neq 0$ if $m \neq 0$, such that $\tau(m_1) \geq \tau(m_2)$ iff $w(m_1) \geq w(m_2)$. Then the generating sets $\{b_1, \ldots, b_t\}$ that minimize $\sum_{i=1}^t \tau(b_i)$ are precisely those whose $w$-profile is the minimal element of $\text{Prof}(M)$.

Example 2.8. Take $R = \mathbb{Z}/p^r \mathbb{Z}$, with $M$ and $w$ to be arbitrary. Taking $\tau$ to be the function $p^w$ and applying Corollary 2.4 and Corollary 2.7 shows that choosing a generating set $\{m_1, \ldots, m_t\}$ of $M$ that minimizes $\sum_{i=1}^t w(m_i)$ is the same as choosing a generating set $\{m'_1, \ldots, m'_t\}$ of $M$ that minimizes $\sum_{i=1}^t p^{w(m'_i)}$ (or equivalently, that minimizes $\sum_{i=1}^t (p^{w(m'_i)} - 1)$).

3. Codes and the Brauer Group

In this section we will prove Theorem 1.6 which gives formulas for bounds on the essential dimension of $G/\mu$ involving the weights of elements of the associated code $\overline{C}_\mu$.

For an algebraic group $R/k$, a diagonalizable central subgroup $C \leq R$ and a character $\chi \in X(C)$, let $\text{Rep}^C_k(R)$ denote the category of $k$-representations of $G$ such that $C$ acts by $\chi$. We recall the following theorem from [KM08].

Theorem 3.1. [KM08, Theorem 4.4 & Remark 4.5] or [M13, Theorem 6.1] Let $1 \to D \to H \to H/D \to 1$ be an exact sequence of algebraic groups with $D$ central and diagonalizable in $H$, and let $d_K : H^1(K,H/D) \to H^2(K,D)$ be the coboundary map for any $K/k$.

- $(1)$ For any $K/k$, $E \in H^1(K,\overline{H})$ and $\chi \in X(D)$ we have
  $$\text{ind}(\chi_* \circ d_K(E)) \mid \gcd\{\dim(V) \mid V \in \text{Rep}^\chi_D(H)\}$$

- $(2)$ There exists a field $K/k$ and $E \in H^1(K,H/D)$ such that for any $\chi \in X(D)$ we have
  $$\text{ind}(\chi_* \circ d_K(E)) = \gcd\{\dim(V) \mid V \in \text{Rep}^\chi_D(H)\}$$

Recall that $p^{\mu}$ and $p^{\beta}$ were defined to be the maximum index and exponent respectively of $\delta_k^i(E)$ over all $E \in H^1(K,\overline{G}_i)$ and $K/k$. We now prove a lemma which says that they can both be attained by the same torsor.

Lemma 3.2. For each $i$, there exists $K/k$ and $E \in H^1(K,\overline{G}_i)$ such that $\text{ind}(\delta_k^i(E)) = p^{\mu_i}$ and $\text{exp}(\delta_k^i(E)) = p^{\beta_i}$.

Proof. Let $V$ be a generically free representation of $\overline{G}_i$. Then there exists a ‘friendly’ subset $U \subset V$ (see [BF03, Theorem 4.7]), i.e. a dense open $\overline{G}_i$-invariant subset $U \subset V$ such that the categorical quotient $U/\overline{G}_i$ exists and $U \to U/\overline{G}_i$ is a $\overline{G}_i$-torsor. Then the generic fiber of this $\overline{G}_i$-torsor gives a $G_i$ torsor $E$ with base $K = k(U/\overline{G}_i)$ (i.e. $E \in H^1(K,\overline{G}_i)$). By [GMS03, Example 5.4], $E$ is versal.
By Theorem 3.1, \( \text{ind}(\delta_K^i(E)) \) is the maximum value of \( \text{ind}(\delta_L^i(A)) \) over all \( L/k \) and \( A \in H^1(L, \mathcal{G}_i) \), i.e. \( \text{ind}(\delta_K^i(E)) = p^{\alpha} \).

Let \( p^\alpha \) be the exponent of \( \delta_K^i(E) \in \operatorname{Br}(K) \). Consider the natural transformation

\[
H^1(-, \mathcal{G}_i) \xrightarrow{\delta^i} H^2(-, Z(G_i)) \xrightarrow{P} H^2(-, Z(G_i))
\]

where \( P \) is the map sending \( A \) to \( A^{\otimes p^\alpha} \) for any \( A \in H^2(L, Z(G_i)) \) and any \( L/k \). This natural transformation is a cohomological invariant of \( \mathcal{G}_i \), and in fact lands in \( H^2(-, \mu_{p^\alpha}) \subset H^2(-, Z(G_i)) \).

By construction, this invariant evaluates to the class of zero when applied to the versal torsor \( E \in H^1(K, \mathcal{G}_i) \) and hence by [GM03, Theorem 12.3], the invariant is identically zero. In particular, \( \delta_K^i(E) \) has maximal exponent over all \( L/k \) and \( A \in H^1(L, \mathcal{G}_i) \), and hence \( b_i = c_i \) as required. \( \square \)

Consider the sequence \( 1 \to Z(G)/\mu \to G/\mu \to G \to 1 \). For any \( K/k \) and \( E \in H^1(K, \mathcal{G}) \) we have a map \( \Psi_{E,K} : C_\mu \to \operatorname{Br}(K) \) given by

\[
\Psi_{E,K} : C_\mu \to \operatorname{Br}(K) \\
\chi \mapsto \chi_* \circ \delta_K(E)
\]

where \( \delta_K \) denotes the coboundary map \( H^1(K, \mathcal{G}) \to H^2(K, Z(G)/\mu) \).

**Remark 3.3.** If \( c = (c_1, \ldots, c_r) \in C_\mu \), \( \delta_{E}^i : H^1(K, \mathcal{G}_i) \to H^2(K, Z(G_i)) \), and \( E = (E_1, \ldots, E_r) \in H^1(K, \mathcal{G}) \) with each \( E_i \in H^1(K, \mathcal{G}_i) \), then it is easy to verify that

\[
\Psi_{E,K}(c) = [\delta_{E}^1(E_1)^{\otimes c_1} \otimes \cdots \otimes \delta_{E}^r(E_r)^{\otimes c_r}].
\]

In particular, the index of \( \Psi_{E,K}(c) \) is a power of \( p \) for any \( c \in C_\mu \), and \( \Psi_{E,K} \) factors through \( \overline{\Psi_{E,K}} : \overline{C_\mu} \to \operatorname{Br}(K) \) by definition of \( \overline{C_\mu} \).

We define \( T_{E,K} \leq \operatorname{Br}(K) \) to be the (finite) image of \( \Psi_{E,K} \). Let \( \{x_1, \ldots, x_l\} \) be a generating set of \( T_{E,K} \) with \( \sum_{i=1}^l \text{ind}(x_i) \) minimal, and define

\[
\text{ind}(E, K) = \left( \sum_{i=1}^l \text{ind}(x_i) \right) - l
\]

**Theorem 3.4.** Let \( \mu \leq Z(G) \), and for any character \( \chi \in C_\mu \), let \( \overline{\chi} \) denote its image in \( \overline{C_\mu} \). Then

1. For any field \( K/k \) and \( E \in H^1(K, \mathcal{G}) \), and \( \chi \in C_\mu \) we have \( \text{ind}(\Psi_{E,K}(\chi)) \leq p^w(\overline{\chi}) \).
2. There exists a field \( K/k \) and \( E \in H^1(K, \mathcal{G}) \) such that for any \( \chi \in C_\mu \) we have \( \text{ind}(\Psi_{E,K}(\chi)) = p^w(\overline{\chi}) \).
3. Let \( Y \) be a minimal generator matrix for \( \overline{C_\mu} \) with rows \( Y_1, \ldots, Y_t \). Then

\[
\max_{E,K}(\text{ind}(E, K)) = \left( \sum_{i=1}^t p^w(Y_i) \right) - t
\]

**Proof.**

1. For any \( K/k \), \( E = (E_1, \ldots, E_r) \in H^1(K, \mathcal{G}) \), and \( \chi \in C_\mu \) with \( \overline{\chi} = (\overline{c}_1, \ldots, \overline{c}_r) \in \overline{C_\mu} \), by Remark 3.3 and Remark 1.4 we have

\[
\text{ind}(\Psi_{E,K}(\chi)) = \text{ind}(\overline{\Psi_{E,K}(\chi)}) = \text{ind}(E_1^{\otimes \overline{c}_1} \otimes \cdots \otimes E_r^{\otimes \overline{c}_r}) \leq p^w(\overline{\chi}).
\]

2. We may assume that \( k \) is algebraically closed. By Theorem 3.1 we can find \( K/k \) and \( E \in H^1(K, \mathcal{G}) \) such that for all \( \chi \in C_\mu \),

\[
\text{ind}(\Psi_{E,K}(\chi)) = \gcd \left( \dim(V) \mid V \in \mathbb{R}_{Z(G)/\mu}(G/\mu) \right)
\]
and since we are studying only reductive groups in characteristic zero, this can be rewritten as
\[ \text{ind}(\Psi_{E,K}(\chi)(E)) = \gcd \left\{ \dim(V) \mid V \text{ irreducible, } V \in \Rep_{Z(G)/\mu}^X(G/\mu) \right\}. \]

If \( \chi \in C_\mu \), then via the inclusion \( C_\mu \hookrightarrow X(Z(G)) \) we can view \( \chi \in X(Z(G)) \). We can view a representation of \( G/\mu \) as a representation of \( G \) via the morphism \( G \to G/\mu \). If \( V \) is a representation of \( G \) such that \( Z(G) \) acts by \( \tau \in X(Z(G)) \), then it is easy to see that \( V \) is a well-defined representation of \( G/\mu \) precisely when \( \tau \in C_\mu \). It follows that for any \( \chi \in C_\mu \), the functor
\[ F : \Rep_{Z(G)/\mu}^X(G/\mu) \to \Rep_{Z(G)}^X(G) \]
is an isomorphism of categories. Thus
\[ \text{ind}(\Psi_{E,K}(\chi)) = \gcd \left\{ \dim(V) \mid V \text{ irreducible, } V \in \Rep_{Z(G)}^X(G) \right\} \]

Since \( k \) is algebraically closed, a representation \( V \) of \( G \) decomposes as \( V = V_1 \otimes \cdots \otimes V_r \), where \( V_i \) is an irreducible representation of \( G_i \) for \( i = 1, \ldots, r \). If \( \chi = (c_1, \ldots, c_r) \in C_\mu \) then \( Z(G_i) \) acts on \( V_i \) by the character \( (c_j) \in X(Z(G_i)) \).

If \( J_i \) is any set of integers for \( 1 \leq i \leq r \), then one can easily check the following gcd result:
\[ \gcd_{J_i \in J_i, i = 1, \ldots, r} \{ j_1 \cdot \ldots \cdot j_i \} = \gcd_{J_i \in J_i} \{ j_1 \} \cdot \ldots \cdot \gcd_{J_i \in J_i} \{ j_r \} \]

Applying this result with \( J_i = \{ \dim(V_i) \mid W \in \Rep_{Z(G_i)}^e(G_i) \} \), (1) reduces to:
\[ \text{ind}(\Psi_{E,K}(\chi)) = \prod_{i=1}^r \left( \gcd \left\{ \dim(V_i) \mid V_i \text{ irreducible, } V_i \in \Rep_{Z(G_i)}^e(G_i) \right\} \right). \]

By Lemma 3.2 there exists \( K/k \) and \( T_i \in H^1(K, G_i) \) such that \( \text{ind}(\delta_{K}^e(T_i)) = p^{a_i} \) and \( \exp(\delta_{K}^e(T_i)) = p^h \). By Remark 1.4 if \( c_i \) is the reduction of \( c_i \) mod \( p^h \), then \( \text{ind}(\delta_{K}^e(T_i)^{\otimes c_i}) = p^{a_i - v_i(\overline{c_i})} \). Note that \( \delta_{K}^e(T_i)^{\otimes c_i} = c_i \circ \delta_{K}^e(T_i) \), and so by Theorem 3.1 applied to the exact sequence \( 1 \to Z(G_i) \to G_i \to G_i \to 1 \),
\[ \gcd \left\{ \dim(V_i) \mid V_i \text{ irreducible, } V_i \in \Rep_{Z(G_i)}^{c_i}(G_i) \right\} \]
is at least as large as \( \text{ind}(\delta_{K}^e(T_i)^{\otimes c_i}) \). Thus we have
\[ \gcd \left\{ \dim(V_i) \mid V_i \text{ irreducible, } V_i \in \Rep_{Z(G_i)}^{c_i}(G_i) \right\} \geq p^{a_i - v_i(\overline{c_i})} \]
and hence,
\[ \text{ind}(\Psi_{E,K}(\chi)) \geq \prod_{i=1}^r p^{a_i - v_i(\overline{c_i})} = p^{\sum_{i=1}^r (a_i - v_i(\overline{c_i}))} = p^{w(\overline{\chi})}. \]

Part 2 now follows by applying part 1.

(3) Since \( \{ \Psi_{E,K}(Y_1), \ldots, \Psi_{E,K}(Y_t) \} \) generate \( T_{E,K} \) for any \( K/k \) and \( E \in H^1(K, \overline{G}) \), the inequality
\[ \max_{E,K}(\text{ind}(E, K)) \leq \left( \sum_{i=1}^t p^{w(Y_i)} \right) - t \]
follows immediately from part 1. For the lower bound, choose \( K/k \) and \( E \in H^1(K, \overline{G}) \) satisfying the result of part 2. In this case,
\[ \Psi_{E,K} : \overline{G}_\mu \to T_{E,K} \]
will be an isomorphism, and \( \text{ind}(E, K) \) will be the minimum value of
\[
\sum_{i=1}^{l} \left( p^{w(\chi_i)} \right) - l
\]
over all generating sets \( \chi_1, \ldots, \chi_l \) of \( C_\mu \). By Example 2.8 this value is
\[
\sum_{i=1}^{l} \left( p^{w(Y_i)} \right) - t.
\]
Before using this to prove Theorem 1.6, we first prove the following lemma.

**Lemma 3.5.** Let \( H \) be an algebraic group and \( T \leq H \) such that \( T \) is central and diagonalizable in \( H \), and let \( d_K : H^1(K, H/T) \to H^2(K, T) \) be the coboundary map. Suppose that for any \( \chi \in X(T), K/k \) and \( E \in H^1(K, H/T) \) the index of \( \chi \circ d_K(E) \in \text{Br}(K) \) is a power of \( p \). Let \( T_p \) be the \( p \)-torsion subgroup of \( T \), \( \chi \in X(T_p) \) and \( \chi_i \) be the preimages of \( \chi \) under the natural map \( X(T) \to X(T_p) \). Then
\[
\gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} = \min_{i \in I} \left( \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} \right)
\]
Proof. Since the collection of objects in \( \text{Rep}_{T_p}(H) \) is the union of the objects in \( \text{Rep}_{T_p}(H) \) over all \( i \in I \), using general properties of \( \gcd \) we have
\[
\gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} = \gcd \left( \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} \right)
\]
By Theorem 3.1 for some \( K/k \) and \( E \in H^1(K, H/T) \),
\[
\gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} = \text{ind}(\chi_i \circ d_K(E))
\]
for all \( i \), and hence \( \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{T_p}(H) \right\} \) is a power of \( p \) for all \( i \). Thus we can replace \( \gcd \)
by \( \min \) and the result follows.

We can now prove Theorem 1.6. Throughout the proof, to simplify notation we will write \( \tilde{G} \) for \( G/\mu \).

**Proof of Theorem 1.6.** By Corollary 0.4 we may assume without loss of generality that 
\[
\text{rank}(C_\mu) = \text{rank}(\overline{C_\mu}) = t.
\]
From [M13, Formula (5.3) in Section 5] and [KM08, Theorem 2.1 & Remark 2.9], and applying Corollary 2.5 we have that for any \( K/k, E \in H^1(K, \tilde{G}) \),
\[
\text{cdim}_K([E/\tilde{G}]) = \text{cdim}_K([E/\tilde{G}]; p) = \text{ind}(E, K).
\]
Here, \( \text{cdim}_K([E/\tilde{G}]) \) (resp. \( \text{cdim}_K([E/\tilde{G}]; p) \)) denotes the canonical dimension (resp. \( p \)-dimension) of the quotient stack \( [E/\tilde{G}] \). For more information on canonical dimension and quotient stacks, see [M13, Section 4 & 5].
Since \( \text{ed}_K(Z(G)/\mu) = t - \dim(Z(G)/\mu) \) and
\[
\dim(Z(G)/\mu) = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}
\]
the upper bound follows immediately from [M13, Corollary 5.8], [LO13, Corollary 3.2] and Theorem 3.4.3.
For the lower bound, consider the exact sequence

\[ 1 \to (Z(G)/\mu)_{p} \to \tilde{G} \to Q \to 1 \]

where \((Z(G)/\mu)_{p}\) denotes the \(p\)-torsion subgroup of \((Z(G)/\mu).\) Let \(\delta_{K'} : H^{1}(K', Q) \to H^{2}(K', (Z(G)/\mu)_{p})\) be the cobounday map for any \(K'.\) By Theorem 6.2, we can take \(K'/k\) and \(E' \in H^{1}(K', Q)\) such that

\[ \text{ind}(\tau \circ \delta_{K'}(E')) = \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{(Z(G)/\mu)_{p}}(\tilde{G}) \right\} \]

for all \(\tau \in X((Z(G)/\mu)_{p}).\)

Choose a basis \(\tau_{1}, \ldots, \tau_{m}\) of \(X((Z(G)/\mu)_{p})\) such that \(\sum_{i=1}^{m} \tau_{i} \circ \delta_{K'}(E')\) is minimal. Then by [M13, Theorem 6.2], we have

\[ (2) \quad \text{ed}_{k}(\tilde{G}; p) \geq \sum_{i=1}^{m} \text{ind}(\tau_{i} \circ \delta_{K'}(E')) - \dim(\tilde{G}). \]

By Lemma 3.4.1, we can choose \(\chi_{1}, \ldots, \chi_{m} \in C_{\mu}\) such that the image of \(\chi_{i}\) in \(X((Z(G)/\mu)_{p}) = C_{\mu}/pC_{\mu}\) is \(\tau_{i}\) and

\[ \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{(Z(G)/\mu)}(\tilde{G}) \right\} = \text{ind}(\tau_{i} \circ \delta_{K'}(E')) \]

for \(1 \leq i \leq m.\)

For any character \(\chi \in C_{\mu},\) let \(\overline{\chi}\) denote the image of \(\chi\) in \(C_{\mu}/pC_{\mu}\). By Theorem 6.2, we can choose \(K/k\) and \(E \in H^{1}(K, \overline{\chi})\) such that if \(\chi \in C_{\mu},\) then

\[ \text{ind}(\Psi_{E,K}(\chi)) = p^{w(\overline{\chi})}. \]

Consider the composition

\[ C_{\mu} \xrightarrow{\Psi_{E,K}} T_{E,K} \to T_{E,K}/pT_{E,K}. \]

The kernel of this composition contains \(pC_{\mu}\), and since \(\chi_{1}, \ldots, \chi_{r}\) generate \(C_{\mu}/pC_{\mu}\) the images of \(\chi_{1}, \ldots, \chi_{m}\) generate \(T_{E,K}/pT_{E,K}\). Since \(T_{E,K}\) is a finite abelian \(p\)-group, by Lemma 3.4.1 \(\Psi_{E,K}(\chi_{1}), \ldots, \Psi_{E,K}(\chi_{m})\) generate \(T_{E,K}\). By Lemma 3.1

\[ \text{ind}(\Psi_{E,K}(\chi_{i})) \leq \gcd \left\{ \dim(V) \mid V \in \text{Rep}_{(Z(G)/\mu)}(\tilde{G}) \right\} = \text{ind}(\tau_{i} \circ \delta_{K'}(E')) \]

Thus by (2) and our choice of \(K\) and \(E,\) we have

\[ \text{ed}_{k}(\tilde{G}; p) \geq \sum_{i=1}^{m} \text{ind}(\Psi_{E,K}(\chi_{i})) - \dim(\tilde{G}) = \sum_{i=1}^{m} p^{w(\overline{\chi_{i}})} - \dim(\tilde{G}). \]

Also by our choice of \(K\) and \(E,\) we have that \(\overline{\Psi}_{E,K}\) is an isomorphism, and hence \(\{\overline{\chi_{1}}, \ldots, \overline{\chi_{r}}\}\) generate \(C_{\mu}/pC_{\mu}\). Thus if \(Y_{1}, \ldots, Y_{t}\) are the rows of a minimal generator matrix for \(C_{\mu},\) then by definition of a minimal generator matrix and Example 2.8 we have

\[ \sum_{i=1}^{m} p^{w(\overline{\chi_{i}})} \geq \sum_{i=1}^{t} p^{w(Y_{i})} \]

and thus we get

\[ \text{ed}_{k}(\tilde{G}; p) \geq \sum_{i=1}^{t} p^{w(Y_{i})} - \dim(\tilde{G}). \]
Thus the result follows by observing \( \dim(\tilde{G}) = \dim(G) + d \), where
\[
d = \begin{cases} 
  t, & \text{if } Z(G) \text{ is connected;} \\
  0, & \text{if } Z(G) \text{ is finite.}
\end{cases}
\]

\[ \square \]

**Remark 3.6.** An alternate method to prove the lower bound on \( ed_k(G/\mu; p) \) in Theorem [1.6] would be to find a finite \( p \)-subgroup \( Y \) of \( G/\mu \) and apply the bound
\[
ed_k(G/\mu; p) \geq ed_k(Y; p) - \dim(G/\mu)
\]
(see [BF03 Theorem 6.19]). Suppose that for \( 1 \leq i \leq r \), one can find a finite \( p \)-subgroup \( H_i \leq G_i \) with \( Z(H_i) = \mu_i \) \( \leq Z(G_i) \), and such that the maximal index and exponent of the coboundary map \( H^1(-, H_i/Z(H_i)) \to H^2(-, Z(H_i)) \) are \( p^{a_i} \) and \( p^{b_i} \) respectively. Then set \( H = H_1 \times \cdots \times H_r \) and \( \mu_f = \mu \cap H \) so that we have \( H/\mu_f \leq G/\mu \), and observe that \( C_{\mu_f} = C_{\mu_f} \). Theorem [1.6] applies, and gives \( ed_k(H/\mu_f; p) \geq \sum_{i=1}^t p^{w(Y_i)} \).

Note that, by Corollary 6.3, we may assume \( \text{rank}(C_{\mu_f}) = \text{rank}(C_{\mu_f}) \), and thus we get the following formula.
\[
ed_k(G/\mu; p) \geq \sum_{i=1}^t p^{w(Y_i)} - d - \dim(G)
\]

where \( d = \begin{cases} 
  t, & \text{if } Z(G) \text{ is connected;} \\
  0, & \text{if } Z(G) \text{ is finite.}
\end{cases} \)

This shows that, if one found such subgroups \( H_i \leq G_i \), then the lower bound on \( ed_k(G/\mu; p) \) provided by computing the essential \( p \)-dimension of \( H/\mu_f \) would be at least as good as the lower bound in Theorem [1.6].

Since we are proving a lower bound on \( ed_k(G/\mu; p) \), we may assume that \( k \) contains \( p^th \) roots of unity. Computing the essential \( p \)-dimension of \( H/\mu_f \) can then be done using [KM08 Theorem 4.1], which says that the essential \( p \)-dimension of a finite \( p \)-group over \( k \) equals the minimal dimension of a faithful representation of that group. This is used in [MR10 Theorem 1.2] to give a formula for the essential \( p \)-dimension of a finite \( p \)-group purely in terms of its group structure. For example, in the case \( G_i = \text{GL}_p \), one can take the group \( H_i \) to be any finite non-abelian group of order \( p^3 \), and the inclusion \( H_i \hookrightarrow G_i \) given by any faithful irreducible representation of \( H_i \); see the group \( \Gamma \) defined in the proof of [MR10 Theorem 1.5].

### 4. An Upper Bound

In this section we will prove Theorem [1.8]. Let \( H = \text{GL}(V_1) \times \cdots \times \text{GL}(V_r) \) and \( H' = \text{SL}(V_1) \times \cdots \times \text{SL}(V_r) \) where \( V_i = k^{n_i} \). Then both \( H \) and \( H' \) act naturally on the vector space \( V_{c_1,\ldots,c_r} = V_1^{\otimes c_1} \otimes \cdots \otimes V_r^{\otimes c_r} \) where \( c_1,\ldots,c_r \in \{\pm 1\} \) (here, \( V^{-1} \) denotes the dual of \( V \)). We denote such a representation by \( \rho_{(c_1,\ldots,c_r)} : H \to \text{GL}(V_{c_1,\ldots,c_r}) \).

**Theorem 4.1.** Suppose \( r \geq 3 \), \( 2 \leq n_1 \leq \ldots \leq n_r \) and \( n_r \leq \frac{n_1 \cdots n_r - 1}{2} \). Then the kernel of \( \rho_{(c_1,\ldots,c_r)} \) is central in \( H \), and the action of \( H/\ker(\rho_{(c_1,\ldots,c_r)}) \) on \( V_{c_1,\ldots,c_r} \) is generically free in all but the following exceptional cases:
\( (1) \ r = 3, \ n_1 = 2, \ n_2 = n_3. \)
\( (2) \ r = 4, \ n_1 = n_2 = n_3 = n_4 = 2. \)
\( (3) \ r = 3, \ n_1 = n_2 = n_3 = 3. \)

**Proof.** We first reduce to the case where \((c_1, \ldots, c_r) = (1, \ldots, 1)\). Suppose the theorem is true in this case, and let \((c_1, \ldots, c_r) \in \{\pm 1\}^r\). By choosing bases of \(V_1, \ldots, V_r\), we can identify \(V_i\) with \(V_i^{\otimes c_i}\) (we can take the identity map if \(c_i = 1\)). Define an automorphism:

\[
\sigma : H \to H \\
(h_1, \ldots, h_r) \mapsto (h_1^*, \ldots, h_r^*)
\]

where

\[
h_i^* = \begin{cases} 
    h_i & \text{if } c_i = 1; \\
    (h_i^{-1})^T & \text{if } c_i = -1.
\end{cases}
\]

Now \(\rho_{(c_1, \ldots, c_r)}\) is isomorphic to the representation \(\rho_{(1, \ldots, 1)} \circ \sigma\). Since \(Z(H)\) is a characteristic subgroup, we see that the theorem holds for \(\rho_{(c_1, \ldots, c_r)}\) as well.

Denote \(\rho_{(1, \ldots, 1)}\) and \(V_{(1, \ldots, 1)}\) by \(\rho\) and \(V\) respectively. It remains to prove that the theorem is true for the representation \(\rho\).

By [PS7] Theorem 2, with the conditions in our theorem, the \(H'/Z(H')\) action on \(P(V)\) is generically free. Thus the stabilizer in general position for the \(H'\)-action on \(V\) is central. Since a central element of \(H'\) either acts trivially on \(V\) or non-trivially on all non-zero elements of \(V\), we see that the stabilizer in general position for the \(H'\)-action on \(V\) is equal to the (central) kernel of this action. It remains to extend this result to the \(H\)-action on \(V\).

We may assume \(k = \overline{k}\) for the purposes of checking whether a representation is generically free. Suppose \(v \in V\) is in general position and \(h \in H\) stabilizes \(v\). Write \(h = \lambda \cdot h'\) with \(\lambda \in (k^*)^r\) and \(h' \in H'\). Then we must have \(h'\) acting by scalar multiplication on \(v\), and hence \(h' \mod Z(H')\) stabilizes the image of \(v\) in \(P(V)\). Thus \(h' \in Z(H')\), and hence \(h \in Z(H)\). As before, a central element of \(H\) either acts trivially on \(V\) or acts non-trivially on every non-zero element of \(V\), and so the stabilizer of a point \(v \in V\) in general position equals the (central) kernel of \(\rho\). Thus the \(H/\ker(\rho)\)-action on \(V\) is generically free, as required.

\( \square \)

We can now apply this to the essential dimension of \(G/\mu\), where \(\mu\) is a subgroup of \(Z(G)\) and \(G_i \leq \text{GL}(V_i)\) is a faithful representation of dimension \(n_i\) whose central character is the identity character. In other words, with \(H\) as above we have \(G \leq H\).

Let \(\chi = (c_1, \ldots, c_r) \in \overline{C}_\mu\). For \(1 \leq j \leq r\), define \(\delta_j\) to be the unique integer such that \(\delta_j \equiv c_j \mod p^{b_j}\) and \(-p^{b_j}/2 < \delta_j \leq p^{b_j}/2\). Define a representation \(\rho_\chi\) of \(G\) by

\[
V_\chi = \bigotimes_{i=0}^{r} V_i^{\otimes \delta_j}
\]

where \(V_i^{\otimes 1}\) is the standard representation, \(V_i^{\otimes 0}\) is the trivial representation, and \(V_i^{\otimes -1}\) is the dual representation of \(V_i\).

We define the set \(m(\chi)\) by

\[
m(\chi) = \{i \mid c_i \neq 0\}
\]

**Definition 4.2.** We say that \(\chi = (c_1, \ldots, c_r) \in \overline{C}_\mu\) is **acceptable** if the following conditions hold:

\( (1) \ -1 \leq \delta_j \leq 1\) for \(1 \leq j \leq r\).
\begin{align*}
(2) \quad \max_{i \in m(\chi)} \{a_i\} &< \frac{1}{2} \left( \sum_{j \in m(\chi)} a_j \right) \quad \text{(note this implies } |m(\chi)| \geq 3). \\
(3) \quad \{n_i\}_{i \in m(\chi)} &\neq \{2, n, n\}, \{2, 2, 2, 2\} \text{ or } \{3, 3, 3\}, \text{ for any positive integer } n.
\end{align*}

By Theorem 4.1, if \( \chi \) is acceptable then the stabilizer in general position for \( \rho_\chi \) equals \( \ker \rho_\chi \), and if \( (g_1, \ldots, g_r) \in \ker \rho_\chi \) then \( g_i \in Z(G_i) \) for all \( i \in m(\chi) \).

\textbf{Remark 4.3.} The first condition in the definition of acceptable implies \( \dim(V_\chi) = p^{w(\chi)} \) for any acceptable \( \chi \).

\textbf{Definition 4.4.} Let \( Y \) be a generator matrix for \( C_\mu \) with rows \( Y_1, \ldots, Y_m \). We say that \( Y \) is \textit{acceptable} if each \( Y_i \) is acceptable and \( Y \) has no column of all zeros.

\textbf{Theorem 4.5.} Suppose \( \mu \leq Z(G) \) and \( C_\mu \) has an acceptable generator matrix \( Y \) with rows \( Y_1, \ldots, Y_t \). Then

\[ \text{ed}_k(G/\mu) \leq t \sum_{i=1}^{t} p^{w(Y_i)} - \dim(G) - d \]

where \( d = \begin{cases} 
1, & \text{if } Z(G) \text{ is connected;} \\
0, & \text{if } Z(G) \text{ is finite.}
\end{cases} \)

\textit{Proof.} Let \( z_i = (\hat{y}_i, \ldots, \hat{y}_t) \in X(Z(G)) \) for \( 1 \leq i \leq t \) and let \( \tau \) be the subgroup of \( Z(G) \) such that \( C_\tau \) is generated by \( z_1, \ldots, z_t \). Then by construction \( \overline{C}_\mu = \overline{C}_\tau \), and hence by Corollary 6.4 we have \( \text{ed}_k(G/\mu) = \text{ed}_k(G/\tau) \).

To each \( Y_i \), we have the associated representation \( \rho_{Y_i} : G \rightarrow \text{GL}(V_{Y_i}) \). If \( Y_i \) is acceptable we have that the stabilizer in general position for \( \rho_{Y_i} \) is \( \ker \rho_{Y_i} \). Let \( \rho = \bigoplus_i \rho_{Y_i} \) and let \( (v_1, \ldots, v_t) \) be in general position in \( V = \bigoplus_i V_{Y_i} \). In particular, \( v_i \) is in general position in \( V_{Y_i} \) for all \( i \). Then it follows from the comments after Definition 4.2 that

\[ \text{Stab}_\rho(v) = \bigcap_{i=1}^{r} \text{Stab}_{\rho_{Y_i}} v_i \]

\[ = \bigcap_{i=1}^{r} \ker \rho_{Y_i} \]

\[ \leq Z(G) \]

where for the last containment we use the property that \( Y \) contains no column of all zeros. In particular, the stabilizer in general position for \( \rho \) is \( \ker \rho \leq Z(G) \). Thus by construction we have \( \ker \rho = \tau \), and hence \( \rho \) is a generically free representation of \( G/\tau \). Since \( \dim(V) = \sum_{i=1}^{t} \dim(V_{Y_i}) \), applying [BF03, Proposition 4.11] gives

\[ \text{ed}_k(G/\tau) \leq \sum_{i=1}^{t} \dim(V_{Y_i}) - \dim(G/\tau). \]

Applying Remark 4.3 and observing that \( \dim(G/\tau) = \dim(G) + d \), gives the desired result. \( \Box \)

Notice that a very acceptable generator matrix is acceptable, and hence Theorem 1.8 follows from Theorem 4.5 by applying the lower bound in Theorem 1.6.
5. Central Simple Algebras with Tensor Product of Bounded Index.

Suppose $p$ is a prime, $r \geq 1$, $a_1, \ldots, a_r \in \mathbb{Z}_{\geq 1}$, and $z \in \mathbb{Z}_{\geq 0}$. Consider the functor $\mathcal{F}_{(a_1, \ldots, a_r);z} : \text{Fields}_k \to \text{Sets}$ given by

$$ \mathcal{F}_{(a_1, \ldots, a_r);z}(K) = \left\{ \begin{array}{l} r \text{-tuples } (A_1, \ldots, A_r) \text{ of central simple } K \text{-algebras} \\ \text{up to isomorphism, such that } \deg(A_i) = p^{a_i} \forall i, \\ \text{and ind}(A_1 \otimes \cdots \otimes A_r) \mid p^z. \end{array} \right\} $$

This functor places a restriction on the index of a certain algebra, and is reminiscent of the functor $H^1(-, \text{GL}_{p^a}/\mu_{p^a})$ discussed in the Introduction, which places a restriction on the exponent of a certain algebra:

$$ H^1(K, \text{GL}_{p^a}/\mu_{p^a}) = \left\{ \text{central simple } K \text{-algebras } A \text{ up to isomorphism} \right\} \\
\text{such that } \deg(A) = p^a \text{ and } \exp(A) \mid p^z $$

Projection to the first $r$ algebras sets up an isomorphism of functors:

$$ \mathcal{F}_{(a_1, \ldots, a_r);0} \to \mathcal{F}_{(a_1, \ldots, a_r);z} $$

and thus we may assume $z = 0$. We will also assume $a_1 \leq a_2 \leq \cdots \leq a_r$.

The functor $\mathcal{F}_{(a_1, \ldots, a_r);0}$ classifies $r$-tuples $(A_1, \ldots, A_r)$ of central simple algebras of specified degrees satisfying the splitting condition $A_1 \otimes \cdots \otimes A_r = 1$ in $\text{Br}(K)$. If we ignored the condition that the tensor product is split, we would be left with the functor $\mathcal{T} = H^1(-, \text{PGL}_{a_1}) \times \cdots \times H^1(-, \text{PGL}_{p^{a_r}})$; the essential dimension of this functor satisfies

$$ \text{ed}_k(\mathcal{T}) < p^{2a_1} + \cdots + p^{2a_r}. $$

We will see in Theorem 5.3 below that, unless $a_r \geq a_1 + \cdots + a_{r-1}$ (which is automatic if $r \leq 2$), the leading term in the essential dimension of $\mathcal{F}_{(a_1, \ldots, a_r);0}$ is $p^{a_1 + \cdots + a_r}$. In other words, when trying to descend a tuple of algebras satisfying the splitting condition, enforcing the splitting condition may require significantly more variables than would be needed to just define the algebras individually.

If we set $G_i = \text{GL}_{a_i} (n_i = p^{a_i})$, $G = G_1 \times \cdots \times G_r$, and

$$ \mu = \{ (\lambda_1, \ldots, \lambda_r) \in Z(G) \mid \lambda_1 \cdots \lambda_r = 1 \} $$

then $C_\mu = [1, \ldots, 1]$ and by Theorem 6.1 we have

$$ \mathcal{F}_{(a_1, \ldots, a_r);0} \cong H^1(-, G/\mu). $$

Remark 5.1. One could ask about the functor $\mathcal{F}_{(a_1, \ldots, a_r);z} : \text{Fields}_k \to \text{Sets}$ given by

$$ \mathcal{F}_{(a_1, \ldots, a_r);z}(K) = \left\{ \begin{array}{l} r \text{-tuples } (A_1, \ldots, A_r) \text{ of central simple } K \text{-algebras} \\ \text{up to isomorphism, such that } \deg(A_i) = p^{a_i} \forall i, \\ \text{and ind}(A_1^{\otimes a_1} \otimes \cdots \otimes A_r^{\otimes a_r}) \mid p^z. \end{array} \right\} $$

for some $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$. By Corollary 6.3 if $\alpha_1 \cdot \cdots \cdot \alpha_r$ is coprime to $p$, then this functor is isomorphic to $\mathcal{F}_{(a_1, \ldots, a_r);z}$.

Lemma 5.2. Let $K/k$ be a field extension.

a) If $r = 1$ then $\mathcal{F}_{a_1;0}(K) = \{ pt \}$.

b) If $r \geq 2$ and $a_r \geq \sum_{i=1}^{r-1} a_i$ (which is automatic if $r = 2$), then projection to the first $r-1$ algebras gives an isomorphism

$$ \gamma : \mathcal{F}_{(a_1, \ldots, a_r);0} \to \prod_{i=1}^{r-1} H^1(-, \text{PGL}_{p^{a_i}}). $$
Proof. Part a) is obvious. For part b), a tuple \((A_1,\ldots, A_r)\) in \(\mathcal{F}_{(a_1,\ldots,a_r);0}(K)\) for some field \(K\) is uniquely determined by \(A_1,\ldots, A_{r-1}\), since \(A_r\) is the unique central simple algebra of degree \(p^{a_r}\) whose Brauer class is
\[
(A_1 \otimes \cdots \otimes A_{r-1})^{op}
\]
It follows that \(\gamma\) is injective. To see that \(\gamma\) is surjective, observe that for an arbitrary tuple \((A_1,\ldots, A_{r-1})\) in \(\prod_{i=1}^{r-1} H^1(-,\text{PGL}_{p^{a_i}})\), we have
\[
\text{ind}((A_1 \otimes \cdots \otimes A_{r-1})^{op}) \leq \prod_{i=1}^{r-1} \text{ind}(A_i) \leq p^{a_1+\cdots+a_{r-1}}.
\]
Thus the condition on the \(a_i\)'s guarantees that the Brauer class of
\[
(A_1 \otimes \cdots \otimes A_{r-1})^{op}
\]
will in fact have a representative central simple algebra \(A_r\) of degree \(p^{a_r}\), and thus \((A_1,\ldots, A_{r-1})\) is equal to \(\gamma((A_1,\ldots, A_r))\). \(\square\)

**Theorem 5.3.** If \(r \geq 3\), \(a_r < \sum_{i=1}^{r-1} a_i\), and \((p^{a_1},\ldots, p^{a_r}) \notin \{(2, n, n)_{n \in \mathbb{Z}}, (2, 2, 2), (3, 3, 3)\}\), then
\[
ed_k(\mathcal{F}_{(a_1,\ldots,a_r);0}) = \ned_k(\mathcal{F}_{(a_1,\ldots,a_r);0}; p) = p^{\sum_{i=1}^{r} a_i} - \sum_{i=1}^{r} p^{2a_i} + r - 1
\]

**Proof.** The matrix \([1, \ldots, 1]\) is an acceptable and minimal generator matrix for \(\overline{C_2}\). Since \(\mathcal{F}_{(a_1,\ldots,a_r);0} \cong H^1(-, G/\mu)\) we have
\[
ed_k(\mathcal{F}_{(a_1,\ldots,a_r);0}) = \ned_k(G/\mu)
ed_k(\mathcal{F}_{(a_1,\ldots,a_r);0}; p) = \ned_k(G/\mu; p)
\]
and so the result follows from Theorem [1.8] (and Remark [1.10]). \(\square\)

Now let \(r \geq 3\), and \(a_1 \leq a_2 \leq \cdots \leq a_{r-1}\) such that \((p^{a_1},\ldots, p^{a_{r-1}}) \notin \{(2, n)_{n \in \mathbb{Z}}, (3, 3)\}\). Let
\[
a_r = \left(\sum_{i=1}^{r-1} a_i\right) - 1.
\]
Then by Theorem 6.1
\[
\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}(K) = \left\{\text{m-tuples } (A_1,\ldots, A_{r-1}) \text{ of central simple } k\text{-algebras up to isomorphism, such that } \deg(A_i) = p^{a_i} \forall i \text{ and } A_1 \otimes \cdots \otimes A_{r-1} \text{ is not a division algebra.}\right\}
\]

**Corollary 5.4.** Let \(r \geq 3\), and \(a_1 \leq a_2 \leq \cdots \leq a_{r-1}\) such that \((p^{a_1},\ldots, p^{a_{r-1}}) \notin \{(2, n)_{n \in \mathbb{Z}}, (3, 3)\}\). Let \(a_r = \left(\sum_{i=1}^{r-1} a_i\right) - 1\). Then
\[
ed_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}) = \ned_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}; p) = p^{2a_r+1} - \sum_{i=1}^{r} p^{2a_i} + r - 1
\]
Proof. Theorem 5.3 applies, and gives:

\[ \text{ed}_k(\mathcal{F}(a_1, \ldots, a_{r-1}; a_r)) = \text{ed}_k(\mathcal{F}(a_1, \ldots, a_{r-1}; a_r; p)) = \text{ed}_k(\mathcal{F}(a_1, \ldots, a_r; p)) = p^{a_1+\cdots+a_r} - \sum_{i=1}^{r} p^{2a_i} + r - 1 = p^{2a_r+1} - \sum_{i=1}^{r} p^{2a_i} + r - 1. \]

\[ \square \]

In the exceptional case, \( p = 2 \), \( r = 3 \), \( a_1 = a_2 = a_3 = 1 \), we can compute the essential dimension exactly.

**Theorem 5.5.** For \( p = 2 \),

\[ \text{ed}_k(\mathcal{F}(1,1,1;0)) = \text{ed}_k(\mathcal{F}(1,1,1;0;2)) = 3. \]

**Proof.** We begin with the upper bound. Recall by Theorem 6.1 that \( \mathcal{F}(1,1,1;0)(L) \) classifies triples of quaternion algebras \( (Q_1, Q_2, Q_3) \) (up to isomorphism over \( L \)) such that \( Q_1 \otimes Q_2 \otimes Q_3 \) is split. By a theorem of Albert [L05, Theorem III.4.8], since \( Q_1 \otimes Q_2 \) is not a division algebra, we may write \( Q_1 = (a, b) \) and \( Q_2 = (a, c) \). Thus \( Q_3 \cong Q_1 \otimes Q_2 \cong (a, bc) \). Hence the triple \( (Q_1, Q_2, Q_3) \) descends to the field \( K = k(a, b, c) \) while still satisfying the splitting property. Thus \( \text{ed}_k(\mathcal{F}(1,1,1;0)) \leq 3. \)

To prove the lower bound, consider the map

\[ \Gamma : \mathcal{F}(1,1,1;0) \to H^1(-, SO_4) \]
\[ (Q_1, Q_2, Q_3) \mapsto \alpha \]

Here \( \alpha \) is defined to be the quadratic form such that \( \alpha \oplus \mathbb{H} \oplus \mathbb{H} \cong N(Q_1) \oplus -N(Q_2) \) where \( \mathbb{H} = \{1, -1\} \) is the 2-dimensional hyperbolic form. (Equivalently, using the definition of the Albert form given in [L05, p.69], \( \alpha \) is the quadratic form such that \( \alpha \oplus \mathbb{H} \cong A_{Q_1} \oplus A_{Q_2} \) where \( A_{Q_1}, A_{Q_2} \) is the Albert form of \( Q_1 \) and \( Q_2 \).) By the Witt cancellation theorem, \( \alpha \) is unique up to isomorphism.

We can explicitly compute \( \alpha \) as follows, for arbitrary \( K/k \). Suppose \( Q_1 = (a, b) \) and \( Q_2 = (a, c) \) as above. Then

\[ N(Q_1) = \langle \langle -a, -b \rangle \rangle = \langle 1, -a, -b, ab \rangle \]
\[ N(Q_2) = \langle 1, -a, -c, ac \rangle \]

and so

\[ N(Q_1) \oplus -N(Q_2) = \langle 1, -1, -a, -b, c, ab, -ac \rangle. \]

This is isomorphic to

\[ \langle -b, c, ab, -ac \rangle \oplus \mathbb{H} \oplus \mathbb{H}. \]

Thus \( \alpha \cong \langle -b, c, ab, -ac \rangle \). Since \( H^1(K, SO_4) \) classifies 4-dimensional quadratic forms over \( K \) of discriminant 1, it is clear from specializing the values \( a, b \) and \( c \) in our expression for \( \alpha \) that \( \Gamma \) is surjective. Since \( \text{ed}_k(SO_4; 2) = 3 \) (see [RY00, Theorem 8.1 & Remark 8.2]), by [BF03, Lemma 1.9] we have

\[ \text{ed}_k(\mathcal{F}(1,1,1;0;2)) \geq 3. \]

\[ \square \]
6. Appendix: Galois Cohomology of \( G/\mu \). By Athena Nguyen

Galois cohomology is often used to classify isomorphism classes of algebraic objects over a field. More precisely, given an algebraic structure \( A \) over a field \( k \), and \( G = \text{Aut}_k(A) \), then \( H^1(k,G) \) classifies \( k \)-isomorphism classes of algebraic objects \( A' \) that become isomorphic to \( A \) over a separable closure of \( k \). For further background on Galois cohomology, refer to [97] and [B10]. In this appendix, we will study the Galois cohomology of certain algebraic groups and some of its applications. Let \( G_i \) be an algebraic group over \( k \) with \( Z(G_i) \cong \mathbb{G}_m \) for \( 1 \leq i \leq r \), and \( G = G_1 \times \ldots \times G_r \). Denote by \( \mu \) a central subgroup of \( G \), and \( \delta^i_K \) the coboundary map \( H^1(K,G_i) \to H^2(K,Z(G_i)) \) induced from the short exact sequence

\[
1 \to Z(G_i) \to G_i \to \overline{G_i} \to 1.
\]

Let \( m_i \) be the maximal exponent of the image of \( \delta^i_K \), when viewed in \( \text{Br}(K) \). Note that \( m_i \) needs not be a prime power. For such \( \mu \leq Z(G) \), we define

\[
C_\mu = \ker(X(Z(G)) \to X(\mu)),
\]

and \( \overline{C_\mu} \) to be the code obtained from \( C_\mu \) by reducing the \( i \)-th coordinate in each element of \( C_\mu \) modulo \( m_i \).

The main result of this appendix is the following theorem:

**Theorem 6.1.** Let \( \mu \) be a subgroup of the split torus \( Z(G) \). Given an embedding \( \mu \hookrightarrow Z(G) \), we obtain a map \( G/\mu \to \overline{G} \), and hence an induced map in cohomology \( H^1(K,G/\mu) \to H^1(K,\overline{G}) \). Then, the map

\[
H^1(K,G/\mu) \to H^1(K,\overline{G})
\]

is injective, and identifies \( H^1(K,G/\mu) \) with \( r \)-tuples \( (E_1, \ldots, E_r) \), with \( E_i \in H^1(K,\overline{G_i}) \), such that for all \( \chi = (c_1, \ldots, c_r) \in \overline{C_\mu} \),

\[
\delta^1_K(E_1)^{c_1} \otimes \cdots \otimes \delta^r_K(E_r)^{c_r} = 0 \text{ in } \text{Br}(K).
\]

Note that \( \delta^i_K(E_i)^{c_i} \) is always well-defined since \( \exp(\delta^i_K(E_i)) \mid m_i \).

Before proving Theorem 6.1, we first recall some elementary results from Galois cohomology. Throughout, we will identify \( H^2(K,\mathbb{G}_m) \) with \( \prod_{i=1}^r H^2(K,\mathbb{G}_m) \) in the usual way. Moreover, let \( a = (a_1, \ldots, a_r) \in X(\mathbb{G}_m^r) \). Then, the corresponding induced map in cohomology is given by:

\[
a_\chi : \prod_{i=1}^r H^2(K,\mathbb{G}_m) \to H^2(K,\mathbb{G}_m)
\]

\[
(x_1, \ldots, x_r) \mapsto x_1^{a_1} \cdot x_2^{a_2} \cdot \ldots \cdot x_r^{a_r}.
\]

**Proposition 6.2.** Let \( K/k \) be a field extension.

1. If \( i : A \hookrightarrow B \) is injective, where \( A \) and \( B \) are diagonalizable groups, then \( i_* : H^2(K,A) \to H^2(K,B) \) is injective. In particular, we can identify \( H^2(K,A) \) as a subgroup of \( H^2(K,B) \);
2. Suppose \( A \leq \mathbb{G}_m^r \), thus giving \( X(\mathbb{G}_m^r/A) \) a coordinate system. Then, the image of the map \( H^2(K,A) \to H^2(K,\mathbb{G}_m^r) \) identifies \( H^2(K,A) \) with the subgroup of \( H^2(K,\mathbb{G}_m^r) \) consisting of \( r \)-tuples \( (A_1, \ldots, A_r) \) such that for all \( \chi = (c_1, \ldots, c_r) \in X(\mathbb{G}_m^r/A) \),

\[
A_1^{c_1} \otimes \cdots \otimes A_r^{c_r} = 0 \text{ in } H^2(K,\mathbb{G}_m^r).
\]

This appendix is based on a portion of the author’s Masters’ thesis completed at the University of British Columbia and the author would like to gratefully acknowledge the financial support from the Natural Sciences and Engineering Research Council of Canada and the University of British Columbia.
Proof. (1) Let \( j : B \hookrightarrow \mathbb{G}_m^q \) be an embedding. Then, \( A \hookrightarrow j \) \( \mathbb{G}_m^q \), and we get the following diagram in cohomology:

\[
\begin{array}{ccc}
H^2(K, A) & \xrightarrow{i_*} & H^2(K, B) \\
(j \circ i)_* & \downarrow & \\
H^2(K, \mathbb{G}_m^q) & & \\
\end{array}
\]

We will show that \( (j \circ i)_* \) is injective. Note that we may put \( A \) in a short exact sequence:

\[ 1 \to A \to \mathbb{G}_m^q \to \mathbb{G}_m^q/A \to 1, \]

which yields the following long exact sequence in cohomology:

\[ 0 \to H^1(K, A) \to H^1(K, \mathbb{G}_m^q) \to H^1(K, \mathbb{G}_m^q/A) \to H^2(K, A) \to H^2(K, \mathbb{G}_m^q). \]

Since \( \mathbb{G}_m^q/A \) is a split torus, it follows from Hilbert’s Theorem 90 that \( H^1(K, \mathbb{G}_m^q/A) \) is trivial. Thus, from the long exact sequence in cohomology, we get that the map \( (j \circ i)_* : H^2(K, A) \to H^2(K, \mathbb{G}_m^q) \) is injective, and consequently, so is \( i_* \).

(2) From \( 1 \to A \to \mathbb{G}_m^q \xrightarrow{p} \mathbb{G}_m^q/A \to 1 \), we get the induced sequence in cohomology:

\[ H^2(K, A) \to H^2(K, \mathbb{G}_m^q) \to H^2(K, \mathbb{G}_m^q/A). \]

By part (1), we can identify the image of \( H^2(K, A) \) with \( \ker(p_*) \). Let \( Y = (Y_1, \ldots, Y_r) \) be an element of \( H^2(K, \mathbb{G}_m^q) \). Since \( \mathbb{G}_m^q/A \) is diagonalizable, \( p_*(Y) = 0 \) if and only if \( \chi_*(p_*(Y)) = 0 \) for all \( \chi \in X(\mathbb{G}_m^q/A) \), and since \( \chi_*(p_*(Y)) = Y_1^{\otimes a_1} \cdots Y_r^{\otimes a_r} \), the result follows. \( \square \)

Proof of Theorem 6.4. Consider the following diagram:

\[
\begin{array}{ccc}
1 & \xrightarrow{\tau} & Z(G) \\
\downarrow & & \downarrow \pi \\
1 & \xrightarrow{\tau} & Z(G)/\mu \to G/\mu \to \prod_{i=1}^r \mathbb{G}_i \to 1
\end{array}
\]

Since \( Z(G)/\mu \) is a split torus, we can use a long exact sequence in cohomology and Hilbert’s Theorem 90 to get the following diagram with exact rows:

\[
\begin{array}{ccc}
H^1(K, \prod_{i=1}^r \mathbb{G}_i) \xrightarrow{(\delta_1^K, \ldots, \delta_r^K)} H^2(K, Z(G)) & \xrightarrow{\pi_*} & H^1(K, \prod_{i=1}^r \mathbb{G}_i) \xrightarrow{\delta_k^K} H^2(K, Z(G)/\mu) \\
\downarrow & & \downarrow \\
0 & \to & H^1(K, G/\mu) \xrightarrow{\pi_*} \to 0
\end{array}
\]

By [S27], I.5, Proposition 42, \( \pi_* \) is injective. Thus, we may identify \( H^1(K, G/\mu) \) with the set of \( r \)-tuples \( (E_1, \ldots, E_r) \), where \( E_i \in H^1(K, \mathbb{G}_i) \) for all \( i \), and \( (\delta_1^K(E_1), \ldots, \delta_r^K(E_r)) \in \ker(\tau_*) \). From the exact sequence:

\[ 1 \to \mu \to Z(G) \xrightarrow{\tau} Z(G)/\mu \to 1, \]

we have that \( \ker(\tau_*) = \text{im}(H^2(K, \mu) \to H^2(K, Z(G))) \), which we can identify with the image of the map \( H^2(K, \mu) \to H^2(K, \mathbb{G}_m^q) \) when viewed inside \( \text{Br}(K)^r \). Since the exponent of \( \delta_k^K(E_i) \) divides \( m_i \) and \( \mathbb{G}_\mu \) is obtained from \( C_\mu \) by reducing the \( i \)-th coordinate modulo \( m_i \), the result follows from Proposition 6.212. \( \square \)
Before stating the corollary, we first introduce the following notion of equivalence of codes:

**Definition 6.3.** Two codes are called (linearly) equivalent if one can be obtained from the other by repeatedly performing the following operations:

1. Permuting entries $i$ and $j$ in every vector of the code, for any $i, j$ with $G_i \cong G_j$.
2. Multiplying the $i$th entry in every vector of the code by any $\lambda \in (\mathbb{Z}/p^b\mathbb{Z})^*$, for all $i$ with $G_i \cong \text{GL}_{n_i}$.

Then, using Theorem [6.1], we can prove the following result:

**Corollary 6.4.** Let $\mu, \tau \leq \mathbb{Z}(G)$ and $K/k$. If $\mathcal{C}_\mu$ is equivalent to $\mathcal{C}_\tau$, then there is an isomorphism of functors $H^1(-, G/\mu) \to H^1(-, G/\tau)$. In particular, $\text{ed}_k(G/\mu) = \text{ed}_k(G/\tau)$.

**Proof.** If $\mathcal{C}_\mu = \mathcal{C}_\tau$, then the result is immediate from Theorem [6.1]. Using the definition of equivalence of codes and induction, it suffices to consider the following two cases. In the case that $C_\mu$ is obtained from $C_\tau$ by permuting entries $i$ and $j$ in every vector of the code, for any $i, j$ with $G_i \cong G_j$, the automorphism which swaps $G_i$ with $G_j$ sets up an isomorphism $G/\mu \cong G/\tau$, and the result follows. On the other hand, suppose that $C_\mu$ is obtained from $C_\tau$ by multiplying the $i$th entry in every vector of the code by some $\lambda \in (\mathbb{Z}/p^b\mathbb{Z})^*$, for all $i$ with $G_i \cong \text{GL}_{n_i}$. Using the description of $H^1(K, G/\mu)$ given by Theorem [6.1], one can check that the map

$$H^1(K, G/\mu) \to H^1(K, G/\tau)$$

$$(E_1, \ldots, E_r) \mapsto (E_1, \ldots, E_{i-1}, [E_i^\otimes \lambda], E_{i+1}, \ldots, E_r)$$

is an isomorphism. Here, $[E_i^\otimes \lambda]$ means the algebra of degree $n_i$ which is Brauer equivalent to $E_i^\otimes \lambda$ (such an algebra is unique up to isomorphism). □

**References**


Department of Mathematics, University of British Columbia, Vancouver, BC, Canada, V6T 1Z2
E-mail address: scernele@math.ubc.ca, athena@math.ubc.ca